

ONE HUNDRED FIFTEENTH CONGRESS  
**Congress of the United States**  
**House of Representatives**

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING  
WASHINGTON, DC 20515-6115

Majority (202) 225-2927  
Minority (202) 225-3641

August 27, 2018

Kirstjen Nielsen  
Secretary  
U.S. Department of Homeland Security  
3801 Nebraska Avenue, N.W.  
Washington, DC 20528

Dear Secretary Nielsen:

On March 31, 2017, the Committee on Energy and Commerce opened an investigation into the Common Vulnerabilities and Exposures (CVE) program in response to reports that it was experiencing difficulties in fulfilling its purpose and meeting stakeholder needs.<sup>1</sup> Specifically, media reports revealed that requests for CVE numbers for vulnerabilities reported to MITRE either were taking several weeks or months to process, or were going unanswered.<sup>2</sup> Other individuals and organizations seeking CVE numbers were told their vulnerabilities were “out of scope” and accordingly rejected from the program.<sup>3</sup> This was—and remains—troubling because, as the standardized mechanism which organizations across the globe, including many federal government agencies and private sector stakeholders within the Committee’s jurisdiction, rely upon to identify and share information on cybersecurity vulnerabilities, the CVE program has become critical cyber infrastructure.

Based on the results of the Committee’s investigation thus far, we believe two reforms to the program should be considered. First, the Committee recommends that the federal agency responsible for the program, the Department of Homeland Security (DHS), transition it from a contract-based funding model to a dedicated Program, Project, or Activity (PPA) line item in its annual budget. Second, the Committee recommends that both DHS and MITRE, the Federally Funded Research and Development Center (FFRDC) that has managed the CVE program since

---

<sup>1</sup> Letter from the Hon. Greg Walden, Hon. Tim Murphy, Hon. Marsha Blackburn, and Hon. Robert E. Latta, H. Comm. On Energy and Commerce, to Mr. Jason Providakes, President and Chief Executive Officer, MITRE Corp. (March 31, 2017); Letter from the Hon. Greg Walden, Hon. Tim Murphy, Hon. Marsha Blackburn, and Hon. Robert E. Latta, H. Comm. On Energy and Commerce, to the Hon. General John F. Kelly, Sec’y, U.S. Dep’t of Homeland Security (March 31, 2017).

<sup>2</sup> *Id.*

<sup>3</sup> *Id.*

its inception in 1999, perform biennial reviews of the program to ensure its stability and effectiveness. Without such reforms, the problems revealed through the Committee's document request and outlined in this letter are likely to reoccur.

## **I. The Committee's Document Request**

To better understand and evaluate the challenges facing the CVE program, the Committee requested documents from MITRE and DHS.<sup>4</sup> The Committee requested three sets of documents.

### **a. All Contracts Associated with the CVE Program, Including Any Changes, Amendments, or Associated Modifications**

The Committee first sought all contracts associated with the CVE program, including any changes, amendments, or associated modifications. The CVE program is entirely contract-dependent, so this documentation was key to understanding any problems related to the reliability and stability of the program. Unlike related cybersecurity functions or programs like Continuous Diagnostics and Mitigation (CDM), the National Cybersecurity Protection System (better known as EINSTEIN), or the Computer Emergency Readiness Team (CERT), DHS does not provide a dedicated PPA line item for the CVE program in its annual budget.<sup>5</sup>

Instead, program requirements and funding levels are provided through individual contract awards and modifications, all of which are provided to MITRE under an overarching contract vehicle.<sup>6</sup> Each contract may provide a different funding level for personnel and equipment or include different program goals. As a result, the strength of the CVE program's operation can vary widely based on the details included in each contract award or modification.

With this in mind, the Committee examined the documents produced by both DHS and MITRE, and discovered several concerning facts. Over the nearly seven-year period for which the Committee received contract documentation, that documentation showed:

- The contract vehicle for the CVE program was awarded or modified 30 times;
- Each contract was modified an average of four times over the course of its lifetime;
- Neither the contract award nor the modification dates occurred on a reliable schedule. In fact, the period of time between contract modifications varied acutely;<sup>7</sup>

---

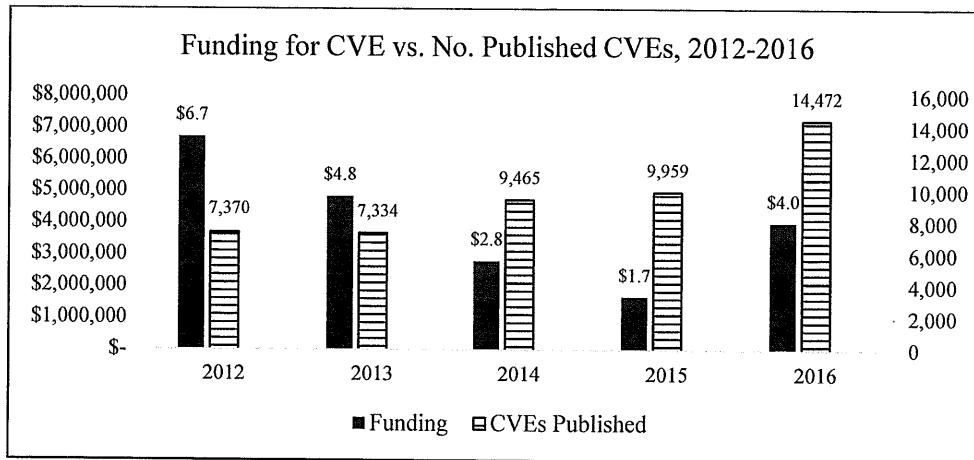
<sup>4</sup> *Id.*

<sup>5</sup> DEP'T OF HOMELAND SEC., NAT'L PROT. AND PROGRAMS DIRECTORATE, BUDGET OVERVIEW, FISCAL YEAR 2019 CONG. JUSTIFICATION, <https://www.dhs.gov/sites/default/files/publications/National%20Protection%20and%20Programs%20Directorate.pdf>.

<sup>6</sup> Documents on file with the Committee.

<sup>7</sup> For example, the shortest span of time between a non-administrative contract action was two days. The longest was 478 days.

- The funding for the program varied acutely, and the amount of money allocated in one contract was not repeated in subsequent contracts,<sup>8</sup> and
- As illustrated in the chart below, from 2012 to 2015, the program received on average 37 percent less year-over-year funding. In 2016, the program received a 139 percent increase in funding.<sup>9</sup>



The documentation produced by DHS and MITRE shows that the CVE contract vehicle is both unstable and prone to acute fluctuations in schedule and funding. As a result, the Committee finds it difficult to imagine how officials responsible for the program were expected to maintain a stable and effective program. Such a haphazard funding schedule requires officials to focus on the CVE program’s short-term needs – to the detriment of medium- and long-term planning – and severely hampers their ability to identify opportunities to evolve the program or to recognize and address program challenges before they become entrenched. Further, even if program officials were to develop such medium- and long-term strategies, they would have no way of knowing if the requisite funding would be provided or, if granted, when it would be available.

**b. Timelines of Actions Taken by DHS and MITRE to Oversee the Management and Fulfillment of the Contract from January 1, 2011, to March 31, 2017**

The Committee next requested timelines from both DHS and MITRE detailing the actions both organizations took to oversee the management and fulfillment of the CVE contract from January 1, 2011, to March 31, 2017. By examining these timelines, the Committee sought to understand how DHS and MITRE ensured that the CVE program remained effective and stable.

<sup>8</sup> For example, starting in 2012 when the contract vehicles became dedicated solely to the CVE program, the lowest amount awarded through a single contract with no modifications, was slightly less than \$1 million. The highest amount awarded was nearly \$7 million, allotted through a contract that was modified four times.

<sup>9</sup> The contract award amounts are rounded to the nearest 100,000<sup>th</sup> place.

Both DHS and MITRE produced copies of “Status Reports” for each awarded contract. These Status Reports detailed the number of CVEs added to the database over the course of the contract, as well as the number of organizations and products that became “CVE compatible” during that same period. Lastly, the Status Reports listed and described press articles that mentioned or otherwise highlighted the CVE program. These Status Reports did not include other information related to specific oversight actions that either DHS or MITRE took during the nearly seven-year period for which the Committee received documentation.

In addition to the Status Reports, and in direct response to the Committee’s request, MITRE developed and produced a specific timeline to highlight actions it took from January 1, 2011, to March 31, 2017, regarding the CVE program. This timeline shows MITRE recognized many of the stakeholder concerns that became the subject of a series of 2016 press reports.<sup>10</sup> But actions MITRE took prior to the publication of the reports were apparently insufficient to preempt or otherwise prevent these concerns from manifesting.

**c. Descriptions and Copies of Any Analyses of the CVE Program Completed by or for Either DHS or MITRE, Including, but not Limited to, Analyses Examining the Performance of the Program, Resource Needs, and Future Requirements to Maintain an Effective and Stable Program, if They Existed**

Lastly, the Committee requested copies of any analyses performed by or for either DHS or MITRE examining the performance, resource needs, and future requirements of the CVE program. For a program that constitutes such a vital piece of critical cyber infrastructure, the Committee expected that both DHS and MITRE would have carried out occasional analyses of the CVE program to ensure its continued effectiveness and stability. However, the Committee did not receive any documentation responsive to this request from DHS.

MITRE produced three slide decks prepared by MITRE and presented to DHS, one from 2013 and two from 2015. While each deck mentioned identified or anticipated issues with the CVE program, these discussions were generally limited to between one to three slides, and did not provide in-depth or root-cause analyses that would help guide the program forward. No other analyses, such as technical or performance audits, white papers, or other responsive documentation were produced. Notably, no such presentation appears to have occurred after the 2016 press reports regarding the length of time it took to process requests for CVE numbers, among other issues.

---

<sup>10</sup> Catalin Cimpanu, *CVE System Sees Huge Backlog, Researchers Propose Alternative*, SOFTPEDIA, Mar. 12, 2016, <http://news.softpedia.com/news/cve-system-sees-huge-backlog-researchers-propose-alternative-501665.shtml>; Sean Sposito, *CVE, a key cybersecurity resource, is at risk inside and out*, SAN FRANCISCO CHRONICLE, Mar. 25, 2016, <http://www.sfchronicle.com/business/article/CVE-a-key-cybersecurity-resource-is-at-risk-7107509.php>; CSO, *Over 6,000 vulnerabilities went unassigned by MITRE’s CVE project in 2015*, CSO ONLINE, Sep. 22, 2016, <http://www.csoonline.com/article/3122460/technology-business/over-6000-vulnerabilities-went-unassigned-by-mitres-cve-project-in-2015.html>.

## **II. The Committee's Recommendations**

Given the importance of the CVE program as critical cyber infrastructure, the Committee expected to receive substantially more documentation in response to its request than was produced. While DHS and MITRE provided all requested documentation, and while the contract documentation in particular was instrumental in understanding the state of the CVE program, the Committee was surprised by the dearth of produced analyses, timelines, and other oversight materials documenting the year-over-year health of the program. The Committee finds the lack of documentation produced by DHS and MITRE to be revealing in and of itself. After close analysis of the materials produced to the Committee, we believe the following reforms should be considered.

### **a. DHS Should Transition the CVE Program to a Dedicated PPA Funding Model**

Since the CVE program's inception in 1999, it has become a critical piece of cyber infrastructure and as such, deserves a dedicated funding stream. Funding this key cybersecurity program through piecemeal, short-term contracts does it a disservice. The Committee therefore recommends that DHS should transition from authorizing and funding the CVE program through individual contracts to providing a dedicated PPA line item in the Department's annual budget requests. A dedicated source of funding would mean the program's goals would no longer be dominated by short-term projects that could be accomplished within the small window of time a single contract is active. By making the program's schedule more reliable and stabilizing its funding levels, program officials would be able to develop broader strategies to stabilize, grow, and improve the CVE program.

Transitioning the CVE program to a dedicated PPA would also demonstrate that DHS recognizes the program's value to stakeholders. As a dedicated line item, the CVE program would be on similar footing as other vital DHS cybersecurity initiatives. That transition would also signal to lawmakers and appropriators that the CVE program is an integral part of DHS's efforts to fulfill its statutory duties to protect the nation from cyber threats.

### **b. DHS and MITRE Should Perform Biennial Reviews of the CVE Program to Ensure its Effectiveness and Stability**

The failure to conduct systematic reviews of the CVE program on a regular basis has allowed small problems to fester and morph into the kind of entrenched problems that the Committee highlighted in its first letter. To stave off these issues in the future, DHS and MITRE should develop and implement a system by which they will carry out thorough, documented biennial reviews of the CVE program. Establishing policies and procedures for systematic reviews would increase the chances that such problems are caught and addressed before they begin to significantly detract from the program's operation.

When program officials conduct biennial reviews, they will have time to determine if the CVE program is meeting its goals and evaluate the program against the evolving landscape in which it operates. Since the CVE program's inception, the nature of cybersecurity threats it is

meant to address has drastically evolved. So, too, have stakeholders' needs. Yet the scope and mission of the CVE program have not undergone similar transformation. By conducting regular reviews of the program, officials would be able to develop short, medium, and long-term goals and then evaluate their progress at achieving those goals. This would also enable officials to fully evaluate whether the CVE program is meeting current stakeholder needs, if changes in the industry will necessitate changes to the program, and whether the program's goals can be met by more efficient means.

While DHS and MITRE are best positioned to determine the exact scope and nature of these reviews, the Committee recommends that they include:

- A dependency analysis that identifies what practices, programs, and organizations are dependent on the CVE program, and examines the potential consequences of CVE inefficiency and instability on those stakeholders;
- An analysis targeted at identifying any nascent issues that may affect the stability of the program, and suggestions for addressing them;
- The identification and explanation of short-, medium-, and long-term goals; and,
- An examination of stakeholder needs and an analysis of whether the program is meeting them.

### **III. The Committee's Conclusions**

The CVE program has become inextricably integrated with cybersecurity practices during its nearly 20-year existence. Yet the documentation produced to the Committee suggests that neither DHS nor MITRE fully recognize CVE's status as critical cyber infrastructure. Instead, both organizations continued to manage and fund the program through a series of contracts which themselves were unstable. This approach was perhaps to be expected given that neither organization, according to produced documentation, performed the level of oversight needed to ensure the program continued to fulfill its purpose and meet stakeholder needs.

The historical practices for managing the CVE program are clearly insufficient. Barring significant improvements, they will likely lead again to challenges that have direct, negative impacts on stakeholders across society. The Committee understands and appreciates that DHS and MITRE have already undertaken reforms to try and address the issues that prompted the Committee's initial request. However, many of these reforms target symptoms that stem from what the Committee considers to be underlying root-causes – the contract-based nature of the program and the lack of oversight – which have yet to be addressed. For DHS and MITRE to address these deep-seated issues, they will have to make significant changes to the very foundation of the CVE program.

As such, the Committee requests that you or your designee provide a briefing to Committee staff about the recommendations made in this letter by September 10, 2018. Please

Letter to the Honorable Kirstjen Nielsen  
Page 7

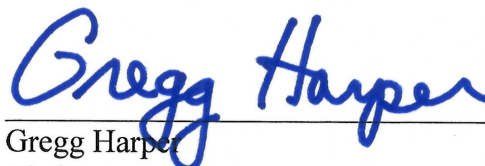
contact Jessica Wilkerson at (202) 225-2927 to schedule this briefing. Thank you for your prompt attention to this request.

Sincerely,



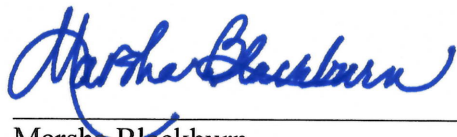
---

Greg Walden  
Chairman



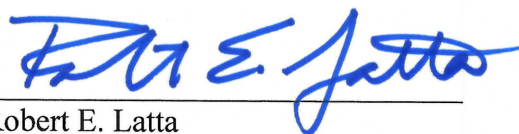
---

Gregg Harper  
Chairman  
Subcommittee on Oversight  
and Investigations



---

Marsha Blackburn  
Chairman  
Subcommittee on Communications  
and Technology



---

Robert E. Latta  
Chairman  
Subcommittee on Digital Commerce  
and Consumer Protection